The purpose of this SAMPLE document is to show in the public domain a typical Conceptual SRS for a "Letdown Station", developed by:

LIUTAIO

"FUNCTIONAL SAFETY SERVICES"

For preparing this SAMPLE report, examples of industrial processes and typical process data was used in combination with

LIUTAIO experience.

However, when this report is prepared for a CUSTOMER, only the authorized or provided information by CUSTOMER will be used, and the report **WILL NOT BE** part of the public domain.

Table of Contents

1. Document purpose

The purpose of this sample document is to show in the public domain a typical "Conceptual SRS" for a "Letdown Station", developed by LIUTAIO "Functional Safety Services".

For preparing this SAMPLE report:

a) Examples of industrial processes and typical process data was used in combination with LIUTAIO experience.

b) "Safety Requirements Specification" (SRS) was developed according to reference [4], 0418D20SD04 Safeguarding requirements - Sample Document, Rev.01.

However, LIUTAIO is a professional and serious company and when this report is prepared for a CUSTOMER, only the authorized or provided information by CUSTOMER will be used, and the report **WILL NOT BE** part of the public domain.

2. Abbreviations

Refer to sample document: 0418D10SD01 Abbreviations

This document additional abbreviations are:

GPP	Gas Processing Plant
LDS	Letdown Station
FCR	Field Control Room
LCR	Local Control Room

3. Glossary

Refer to sample document: 0418D10SD02 Glossary

4. References

[1] LIUTAIO – Functional Safety Services
0418D10SD01 Abbreviations - Sample Document
Rev.01

[2] LIUTAIO – Functional Safety Services
0418D10SD02 Glossary - Sample Document
Rev.01

[3] LIUTAIO – Functional Safety Services
0418D18SD03 SIF General Design Background - Sample Document
Rev.01

[4] LIUTAIO – Functional Safety Services
0418D20SD04 Safeguarding requirements - Sample Document
Rev.01

5. (SRS) Safety Requirements Specification

5.1 SIF Tag number and short description

SIF Tag: 60-SIF-500

Short description: Gas Processing Plant inlet facilities protection against an overpressure operation scenario.

5.2 Hazardous even description that the SIF is protecting from

The Gas Processing Plant (GPP) inlet facilities operate at 7.0 Bar(g), processing gas from production gas wells.

In case of malfunction in one or more wells, or in the production well distribution network, then a big amount of gas can arrive to the GPP, creating a high-pressure operation condition.

To avoid GPP high-pressure operation scenario, high-pressure gas flow is routed through a "Letdown Station" (LDS) before arriving to GPP.

When the pressure @LDS outlet reaches 8.5 Bar(g), 60-SIF-500 shall close ALL safety valves @ LDS, to cut-off feed flow to GPP and therefore stops high-pressure operation condition.

5.3 SIF related process description, operation and actions to achieve the required functional safety

Refer to "APPENDIX A" for 60-SIF-500 simplified diagram for protection of GPP in case of high-pressure operation scenario.

GPP receives high-pressure gas from production gas wells for removing Sulphur, condensate and water; to produce dry gas for commercial distribution. GPP inlet facilities normally operate at 7.0 Bar(g), and this pressure is controlled by a control loop that manipulates all wells' choke valves and other compressors' loads and distribution valves inside the plant.

LDS is designed with four(4) pipe runs. Each run includes a "Quick Shutdown Valve" (QSD) and an "Emergency Shutdown Valve" (ESV). LDS design considered:

a) To normally cut-off flow through LDS, all four(4) pipe runs safety valves shall close.

b) **BUT** in the case one pipe run fails to close, a conventional PRV station is installed downstream of the LDS, which can handle full flow through just one pipe run.

c) Flow cut-off through one(1) pipe run is successful if both ESV and QSV valves are closed.

d) It is possible to operate LDS with only three(3) pipe runs, while one of them is "Out of Service" (OOS, isolated for MAINTENANCE purposes).

e) Safety logic of each pipe run works independently of the safety logic of other pipe runs. It means, each pipe run safety logic decides when to close ESV and QSV valves independently of the other pipe runs,

f) In the same pipe run, the safety logic to trip QSV valve is independent of safety logic to trip ESV valve, and vice-versa.

g) In addition, the high priority trip 60-SIF-510 can trip ALL QSV and ESV valves.

h) De-Energize to Trip philosophy is implemented.

In NORMAL state, ALL LDS's safety valves are opened and the pressure measurement ALL in the LDS's pressure transmitters is around 7.0 Bar(g), but below 8.5 Bar(g).

In SAFE state, 60-SIF-500 for each pipe run shall close the respective safety valves when the respective pipe run outlet pressure transmitter reaches 8.5 Bar(g) or above.

a) The two(2) pressure transmitters on each LDS's pipe run work independently.

b) "Common Logic Solver" (CommonLS) shall monitor both pressure transmitters on each pipe runs.

c) When one pressure transmitter in a pipe run initiates a demand to close (SAFE state) one safety valve, "CommonLS" shall close (SAFE state) the related safety valve associated to the other pressure transmitter in the same pipe run as well.

d) Both safety valves per pipe run shall close (2oo2) to consider that high-pressure gas flow through the pipe run was cut-off successfully.

e) The four(4) pipe runs work in 3oo4 safety architecture.

By design, safety valves in ALL four(4) pipe runs shall close on demand, BUT it is considered that the required safety actions were achieved successfully if high-pressure gas flow is cut-off at least through three(3) pipe runs.

A conventional PRV station is installed downstream of the LDS, which can handle full flow through just one pipe run.

High Priority Trip 60-SIF-510 shall be able to close all QSV and ESV valves in LDS. Only interface between 60-SIF-500/510 is described in this document. Refer to 60-SIF-510 SRS for further information (**NOT** included in this Example development).

The 60-SIF-500 detailed diagram is shown in "APPENDIX B".

All pressure transmitters, solenoid valves and safety valves (ESV & QSV) are in ATEX zone 1 (classified area, safety area). This is the reason Isolators (Barriers) shall be used between field devices and other devices located in Non-classified areas like control room, Field Control Room (FCR), o Local Control Room (LCR).

5.4 SIF Devices' List

Table 1 – 60-SIF-500 Devices' List

#	Device's Tag	Device Type	Input Type	Output Type	Input states		Device data purpose	Device Description
					NORMAL	SAFE		
1	60-PT-511 60-PT-521 60-PT-531 60-PT-541	Initiator		4-20 ma IS, HART, NAMUR NE 43	< 8.5 Bar(g)	≥ 8.5 Bar(g)	SIL & STR	Pipe Run 1, 2, 3 & 4 Quick Shutdown pressure transmitter
2	60-XIB-511 60-XIB-521 60-XIB-531 60-XIB-541	Input	4-20 ma IS, HART pass through, loop powered, NAMUR NE 43	4-20 ma HART pass through, NAMUR NE 43	< 8.5 Bar(g)	≥ 8.5 Bar(g)	SIL & STR	Pipe Run 1, 2, 3 & 4 Quick Shutdown pressure input Barrier/Isolator
3	60-STA-511 60-STA-521 60-STA-531 60-STA-541	Logic	4-20 ma HART, loop powered, NAMUR NE 43	24 VDC	Energized	De-Energized	SIL & STR	Pipe Run 1, 2, 3 & 4 Quick Shutdown Logic Solver

#	Device's Tag	Device Type	Input Type	Output Type	Input states		Device data purpose	Device Description
					NORMAL	SAFE		
4	60-XOB-511 60-XOB-521 60-XOB-531 60-XOB-541	Output	24 VDC	24 VDC, IS, loop powered	Energized	De-Energized	SIL & STR	Pipe Run 1, 2, 3 & 4 Quick Shutdown pressure output Barrier/Isolator
5	60-SOV-511 60-SOV-521 60-SOV-531 60-SOV-541	Output	24 VDC, IS	Pneumatic	Energized	De-Energized	SIL & STR	Pipe Run 1, 2, 3 & 4 SOV to Quick Shutdown Valve
6	60-QSV-511 60-QSV-521 60-QSV-531 60-QSV-541	FSE	Pneumatic		Pressurized, Opened	De-Pressurized, Closed	SIL & STR	Pipe Run 1, 2, 3 & 4 Quick Shutdown Valve
7	60-PT-510 60-PT-520 60-PT-530 60-PT-540	Initiator		4-20 ma IS, HART, NAMUR NE 43	< 8.5 Bar(g)	≥ 8.5 Bar(g)	SIL & STR	Pipe Run 1, 2, 3 & 4 Shutdown pressure transmitter
8	60-XIB-510 60-XIB-520 60-XIB-530 60-XIB-540	Input	4-20 ma IS, HART pass through, loop powered, NAMUR NE 43	4-20 ma HART pass through, NAMUR NE 43	< 8.5 Bar(g)	≥ 8.5 Bar(g)	SIL & STR	Pipe Run 1, 2, 3 & 4 Shutdown pressure input Barrier/Isolator
9	IC-60-PT-510 IC-60-PT-520 IC-60-PT-530 IC-60-PT-540	Input	4-20 ma HART pass through, loop powered, NAMUR NE 43	Logic Solver	< 8.5 Bar(g)	≥ 8.5 Bar(g)	SIL & STR	Pipe Run 1, 2, 3 & 4 Shutdown pressure input card
10	CommonLS	Logic					SIL & STR	Common Logic Solver
11	OC-60-PT-510 OC-60-PT-520 OC-60-PT-530 OC-60-PT-540	Output	Logic Solver	24 VDC	Energized	De-Energized	SIL & STR	Pipe Run 1, 2, 3 & 4 Shutdown pressure output card
12	60-XOB-510 60-XOB-520 60-XOB-530 60-XOB-540	Output	24 VDC	24 VDC, IS, loop powered	Energized	De-Energized	SIL & STR	Pipe Run 1, 2, 3 & 4 Shutdown pressure output Barrier/Isolator
13	60-SOV-510 60-SOV-520 60-SOV-530 60-SOV-540	Output	24 VDC, IS	Pneumatic	Energized	De-Energized	SIL & STR	Pipe Run 1, 2, 3 & 4 SOV to Shutdown Valve
14	60-ESV-510 60-ESV-520 60-ESV-530 60-ESV-540	FSE	Pneumatic		Pressurized, Opened	De-Pressurized, Closed	SIL & STR	Pipe Run 1, 2, 3 & 4 Shutdown Valve

#	Device's Tag	Device Type	Input Type	Output Type	Input states		Device data purpose	Device Description
					NORMAL	SAFE		
15	OC-60SIF510-01 OC-60SIF510-02 OC-60SIF510-03 OC-60SIF510-04	Support	Logic Solver	24 VDC	Energized	De-Energized	ONLY STR	Pipe Run 1, 2, 3 & 4 High Priority Trip 60-SIF-510 output card

Description of column "Device Type" in Table 1:

Initiator	Device that is directly measuring the process variable that can initiate the SIF action.
Input	Device included in the safety input channel, or initiator of the SIF.
Logic	SIF's Logic Solver.
Output	Device included in the safety output channel.
FSE	Final Safety Element

5.5 Safety integrity targets, constraints and other requirements

5.5.1 Safety integrity targets

Table 2 – 60-SIF-500 Safety integrity targets

(Low Demand System)

SIF's Tag number	60-SIF-500	**SIL Verification Report No.**	To be defined
SIF's Description	Gas Processing Plant inlet facilities protection against an overpressure operation scenario		
Process Safety Time (PST)	30 sec	**SIF Response Time (SRT, MART)**	15 sec
Target SIL rating	**SIL 3**	**Maximum SIL Safety Design Limit (MSSDL)**	70%

For Initiators and Trip settings, refer to Table 1.

5.5.2 SIL verification Constraints and default values

Table 3 shows required design constraints and default values for "SIL verification".

Table 3 – 60-SIF-500 SIL verification Constraints and default values

No.	**Description**	**Abbreviation**	**Default value**	**Constraint value**	**Remark**
1	Proof Test Period	TI	12 months	≥ 4 months	
2			12 months	≥ 6 months	ONLY for QSV and ESV valves.
3	Service Life	SLf	10 years	[redacted]	
4	Mean Time To Restoration	MTTR	72 hours	≥ 72 hours	
5	Proof Test Duration	TD	4 hours	≥ 4 hours	
6	Mean Repair Time	MRT	24 hours	≥ 24 hours	

Other constraints shall include:

1) Regarding to calculation of Beta values for "Common Cause Failure" (CCF) effect:

   a) For any "**Decision Logic**" or "**Safety Channel Architecture**" (SCA) equal to "XooN(D)" (N>X and N>1), the CCF effect **MUST BE** calculated. ZERO(0.0) values **ARE NOT** accepted for CCF effect and respective "Beta" (β) values.

      CCF effect is ZERO(0.0) ONLY for "NooN" logic.

   b) Default methodology to calculate Beta values for "Common Cause Failure" (CCF) effect shall be IEC-61508-6, Annex D.

   c) To estimate the CCF effect the "Geometric Average" is the default method to estimate the combined failure rates from devices.

      In a group of devices to consider for CCF effect calculation, when one or some of them has "Dangerous" failure rate (λ_{DD}/LdDD, (λ_{DU}/LdDU) value(s) equal to ZERO(0.0) and other devices **DO NOT**, then the "Geometric Average" shall be applied ONLY to the failure rate values other than ZERO(0.0).

   d) When devices with different "Proof Test Periods" (TI) are involved in the same "Proof Test", the CCF effect calculation MUST BE done to force the CCF's TI to meet each device's TI value.

5.5.3 Other requirements

Other requirements for this SIL verification assessment are described in the following list:

1) "SIL verification" calculations **MUST** consider individual failures of all devices, as well as all possible combined failures, that will make 60-SIF-500 to fail on demand.

2) By default, "SIL verification" shall consider "Fault Detection Capabilities" (Diagnostics) for "Common Logic Solver" (CommonLS) and Input/Output cards.

3) If target SIL rating is no satisfied, propose possible actions/solutions to improve the design of 60-SIF-500.

4) The indicate methodology in above section 5.5.2 point "1.b" shall be used to calculate Beta values for the following cases:

   - SIF **simple** Design/Installation quality is representative of high Beta values (or Worst values).
   - SIF **enhanced** Design/Installation quality is representative of low Beta values (or best values).

   And, "SIL verification" shall be developed by calculating and reporting "Beta" values (β, β_D) corresponding to BOTH the **Simple** (Greater CCF effect) and the **Enhanced** (Lower CCF effect) SIF's Design/Installation cases.

5) Verify SIL rating in the cases of SIF's **simple** and **enhanced** implementation quality, but with **NO** Maintenance effect (MTTR, TD, MRT all equal to 0.0 hours).

6) Verify SIL rating in the same condition as described in above point No.5, but including Maintenance effect (MTTR, TD, MRT).

7) For above point No.6), calculate the SIF's "STRavg" (and "MTTRspurious") in the following cases:

   a) When during normal operation, a "Spurious Trip" occurs in one(1) pipe run.

   b) When during normal operation, a "Spurious Trip" occurs in two(2) pipe runs (**NOT** necessarily at the same time).

   But, using the same point No.4 beta values (Same Common Cause Effect).

8) Since the "Letdown Station" (LDS) can operate with one pipe run "Out of Service" (OOS, for MAINTENANCE purposes), verify that still 60-SIF-500 satisfy the target SIL rating with three(3) pipe runs in operation in 2oo3 configuration.

   NOTE: in this case, use the same beta values that were used for 3oo4 configuration.

9) Repeat calculation above in point No.7) for this point, to determine SIF's "STRavg" (and "MTTRspurious") for 3 pipe runs in operation in 2oo3 configuration.

   NOTE: in this case, use the same beta values that were used for 3oo4 configuration.

5.6 Additional Initiators and Input Channels description

Refer to above Table 1 (60-SIF-500 Devices' List) and "APPENDIX B" (SIF detailed diagram).

The "Initiators":

- 60-PT-511/521/531/541 to trip the QSV valves, and
- 60-PT-510/520/530/540 to trip the ESV valves,

are Smart pressure transmitter (PT), qualified for safe area ATEX Zone 1, intrinsically safe, NAMUR NE 43 capable.

Each PT shall be installed in an instrument manifold that allows MAINTENANCE personnel to:

- Isolate PT from process operation.
- Connect an external gas pressure supply kit to pressurize the transmitter impulse pipe below and above the trip setting (8.5 Bar(g)) for "Proof Test" purposes.
- Equalize pressure to reconnect PT to process operation.
- It **SHALL NOT** be required to disconnect PT or to cut PT power supply to execute above steps.

Manual manipulation of the instrument manifold **SHALL NOT** trip the related safety valve.

Each of the "Input Isolators":

- 60-XIB-511/521/531/541 to trip the QSV valves, and
- 60-XIB-510/520/530/540 to trip the ESV valves,

Shall have:

a) Classification input from Zone 0 or 1, intrinsically safe. HART transparent repeater and NAMUR NE43 capable. Input with Loop powered mode.

b) 1-channel input.

c) 2-channels outputs:

   - ➢ For 60-XIB-511/521/531/541 one output is connected to the respective "Safe Trip Alarm" (STA) module, and the other one is connected to DCS for initiator process variable monitoring and "Asset Management" (ASM) purposes (HART capable).
   - ➢ For 60-XIB-510/520/530/540 one output is connected to the input card at the "Common Logic Solver" (CommonLS), and the other one is connected to DCS for initiator process variable monitoring and "Asset Management" (ASM) purposes (HART capable).

5.7 Manual shutdown requirements

N/A

5.8 Startup Bypass requirements

N/A

5.9 SIF Decision Logic and Calculations

60-SIF-500 includes five(5) "Logic Solvers":

a) The "Common Logic Solver" (CommonLS) to handle four(4) "Decision Logics" that monitor four(4) "Initiators" 60-PT-510/520/530/540 to trip the shutdown valves 60-ESV-510/520/530/540, respectively, and

b) Four(4) additional "Safe Trip Alarm" (STA, Logic Solver) modules to monitor the "Initiators" 60-PT-511/521/531/541 to trip the quick shutdown valves 60-QSV-511/521/531/541, respectively.

When one pressure transmitter in a pipe run initiates a demand to close (SAFE state) the related safety valve, "CommonLS" shall close (SAFE state) the related safety valve associated to the other pressure transmitter in the same pipe run.

If a GPP shutdown happens that cuts the normal gas processing flow inside GPP, then high priority trip 60-SIF-510 activation happens, and this action shall initiate a 50-SIF-600 demand to close (SAFE state) ALL LDS safety valves as well.

5.10 Interlock management requirements

N/A

5.11 Additional "Final Safety Elements" (FSEs) and Output Channels description

ALL "Quick Shutdown Valves" (QSV) and "Emergency Shutdown Valves" (ESV) shall include magnetic limit switches, to detect the closed, opened and travelling valve position.

These magnetic limit switches shall be connected to DCS.

Both QSV and ESV per pipe run are valves of the same size, but with different actuators. QSV shall close faster than ESV.

Each of the "Output Isolators":

- 60-XOB-511/521/531/541 to trip the QSV valves, and
- 60-XOB-510/520/530/540 to trip the ESV valves,

Shall have:

a) Output to Zone 0 or 1. Output with Loop powered mode.

b) 1-channel input.

c) 1-channels output connected to the respective safety valve (QSV or ESV) solenoid (SOV).

Each "Output Isolator" shall be configured to trip in case a "Dangerous Detected" failure occurs.

Refer to below section 5.16.4 for further details.

5.12 Reset function requirements, actions after shutdowns and/or before startup

Refer to references [3] and [4] for "Reset function" description.

One(1) "Manual Reset" (soft-button) shall be implemented in the "Common Logic Solver" (CommonLS) for each LDS pipe run (total 4 buttons). This soft-button HMI shall be implemented in DCS console. Refer to Table 5 for Reset buttons tags.

One "Reset Logic" shall be implemented in the "CommonLS" for each emergency shutdown valves 60-ESV-510/520/530/540, and for each quick shutdown valve 60-QSV-511/521/531/541.

In addition, for each quick shutdown valve 60-QSV-511/521/531/541:

a) The "Manual Reset" (MR) functionality shall be activated in the "Safe Trip Alarm" (STA, Logic Solver) 60-STA-511/521/531/541, respectively, to allow STA to perform the "Reset Logic" functionality by external "RESET command" from "CommonLS",
b) The respective STA "RESET command" signal shall be wired from the "CommonLS" output card to the respective STA module (MR contact). This connection shall be normally De-Energized (NDE).

ALL "Reset Logic" output signals from "CommonLS" shall be in SAFE state after power up.

"CommonLS" and ALL STA modules 60-STA-511/521/531/541 shall be power up at the same time.

STA module shall be configured to retain output in SAFE state (De-Energized) for 5 min after STA power up. In this way, it is guarantee that all quick shutdown valve will remain in SAFE state after "CommonLS" and STA modules power up.

5.13 Operation and DCS HMI, alarms and even messages

Refer to section 4.2.13 in document: (reference [3])

0418D20SD04 Safeguarding requirements - Sample Document

5.14 Integration with Control and operation startup

Before commissioning, ALL "Letdown Station" (LDS) pipe runs shall be isolated and "Out Of service" (OOS state) to facilitate the installation and local testing of LDS instruments.

During LDS commissioning, Console Operator shall dismiss OOS state in all selected pipe runs ready to startup, and ALL safety valves of selected pipe runs shall be closed (SAFE state).

Before LDS startup and GPP feed up, wells' production flowlines network and the "Gas Processing Plant" GPP shall be equalized in pressure and ready to feed up (equal LDS input/output pressure). This is the initial plant safeguarding condition (PERMISSIVE) to initiate LDS startup to open the LDS safety valves.

Once LDS PERMISSIVE is satisfied, to start each LDS pipe run, the Console Operator shall apply Reset to the pipe run and the related safety valves (QSV and ESV) shall open (NORMAL state).

Next, the Console Operator can initiate GPP feed up by opening wells' choke valves.

In case of GPP shutdown, the production wells' choke valves shall be trip as well. In this condition, LDS shall trip only if the settle down pressure of the wells' production flowlines network is at or above 8.5 Bar(g). IF LDS trips, follow the above described procedure to re-start LDS.

If an LDS pipe run "Spurious Trip" occurs, both pipe run safety valves will close (SAFE state) and will remain in the closed position. In this case:

a) If other pipe runs are still running in normal operation (GPP is still running), LDS PERMISSIVE is still satisfied, and Console Operator shall apply Reset to the trip pipe run and the safety valves (QSV and ESV) shall open (NORMAL state).

b) If other pipe runs also trip and GPP also trip, LDS PERMISSIVE **IS NOT** still satisfied, and Console Operator shall follow above described procedure for LDS startup and GPP feed up.

5.15 "Proof Test" requirements and use of MOS

Refer to section 4.2.15, in document (reference [3]) 0418D20SD04 Safeguarding requirements for further MOS information and requirements.

A total of Eight(8) different "Proof Tests" can be performed in the "Letdown Station" (LDS).
Independent "Proof Test" shall be performed for:

1) Each series of devices that trip the quick shutdown valve 60-QSV-511/521/531/541, and
2) For "CommonLS" and each series of devices that trip the shutdown valve 60-ESV-510/520/530/540.

For "Proof Test" description of High Priority Trip 60-SIF-510, involving all LDS safety valves, **IS NOT** included in this document. Refer to 60-SIF-510 SRS for further information (**NOT** included in this Example development).

It shall be considered that the command to Trip the safety valve from the "Initiator" under testing will be issued once the "CommonLS" receives the trip signal.

NOTE: when a "Proof Test" is performed in a pipe run "Initiator", once the "CommonLS" receives the trip signal, the command to close both safety valves (QSV and ESV) in the same pipe run shall be issued simultaneously. Refer to above sections 5.3 (SAFE state) and 5.9.

ONLY "Full Valve Stroke Test" (FVST) will be applied to any QSV or ESV.
"Proof Test" can be applied even though while any other pipe run is in "Out Of service" (OOS) state and isolated for MAINTENANCE purposes.

NO manual shutdown soft-button shall be provided when "Proof Test" is in progress. 60-SIF-600's SRT is too short (15 sec) to allow Console Operator to manually initiate a SIF demand that can avoid the Hazard the SIF is protecting from.

See Table 4 for associated MOS tag for each SIF "Proof Test".

ALL SAFETY and PERMISSION procedures **MUST BE** completed and approved before executing any "Proof Test". Only one(1) "Proof Test" can be executed at the time. During "Proof Test" execution ALL other "Initiator" and SIF devices shall be working in normal condition.

If another MOS is active in the same "MOS Group" where 60-SIF-500 is located, then **NO** "Proof Test" can be executed in 60-SIF-500.

The steps to execute a "Proof Test" (to trip QSV or ESV) are as follow:

1) Activate related MOS tag .
   Associated safety valve **MUST** remain opened (NORMAL state).
   The pressure transmitter under testing still can send trip signal to close safety valve.
   NOTE: ONLY while the MOC tag is activated, a soft-button shall be available for "Console Operator", to let this person to close the safety valve at any time if it is required. Refer to Table 4.

2) MAINTENANCE personnel shall manually isolate and pressurize the "Pressure Transmitter" (PT) to test.
   NOTE: PT signal value change **MUST BE** tested above and below trip setting value.

   NOTE: MAINTENANCE personnel shall verify that PT measurement is equal to the kit supplied pressure. If this **IS NOT** true, then the test shall be manually declared "**Unsuccessful**", and MAINTENANCE shall repair or replace PT.

   NOTE: Refer to above section 5.6. Manual manipulation of the instrument manifold **SHALL NOT** make 60-PT-511/521/531/541 to trip.

3) When the PT signal value reaches the required trip setting, the associated safety valve shall close (SAFE state), and "CommonLS" shall close the other safety valve in the same pipe run.
   The "Proof Test" Fail/Success completion criteria shall be:
   - **SUCCESSFUL** when:
     a) Both safety valves in the pipe run DID close before respective "Safety Response Time" (SRT) expires, and
     b) Both: safety valve under testing and the other safety valve in the same pipe run, shall return to fully opened position (NORMAL state) after PST time expires, without applying "RESET command".

   - **UNSUCCESFUL** when any safety valve in the pipe run:
     a) Any safety valve in the pipe run:
        - DID close after respective "Safety Response Time" (SRT) expires, or
        - **DID NOT** leave the fully opened position, or
        - **DID NOT** open fully after "Process Safety Time" (PST) expires, without applying "RESET command".

   - **FAIL SAFE** when while "Proof Test" was in progress:
     a) High Priority Trip 60-SIF-510 initiates a demand.
     b) A demand is initiated by the other pressure transmitter in the same pipe run where the "Proof Test" is in progress.
     c) A demand is initiated by any other mean, other than the pressure transmitter under testing.

NOTE: for application of this step, LDS startup PERMMISSIVE shall not apply, because GPP is already running. Refer to section 5.14.

4) IF the "Proof Test" was "Successful", then continue with next step.
   ELSE, MAINTENANCE shall determine which device(s) in the test failed and fix the fault before the valve's "Mean Time To Restoration" (MTTR).

5) MAINTENANCE personnel shall re-establish the PT normal operation conditions. This MAINTENANCE activity **MUST NOT** initiate a trip.

6) De-Activate related MOS tag, and both pipe run safety valves (QSV & ESV) shall remain closed (SAFE state).

"Proof Test" shall be monitored in DCS, but not initiated from DCS or control room.

60-SIF-500 "Proof Test" implementation support in DCS shall monitor the test and generate test report/record. Refer to section 4.2.15.1 in document (reference [3]) 0418D20SD04 "Safeguarding requirements" for further information.

5.16 Fault detection capabilities (Diagnostics) and required actions

This section is organized in the following sub-sections:

1) Initiators", Input isolators and "Safety Trip Alarm" (STA) to trip QSVs.
2) "Initiators" and Input isolators to trip ESVs.
3) "CommonLS" and respective Input/Output cards required diagnostics
4) Output isolators' required diagnostics.

5.16.1 Initiators", Input isolators and "Safety Trip Alarm" (STA) to trip QSVs

Each device:

- PTs 60-PT-511/521/531/541,
- Input isolators 60-XIB-511/521/531/541, and

shall be configured to set the device output in SAFE state when a device "Diagnostics" detects that a "Detected Failure" occurred. This failure condition shall be communicated up to the STA module according to NAMUR NE 43.

In addition, the "Safety Trip Alarm" (STA) modules 60-STA-511/521/531/541 shall:

a) After a demand (from PT or own STA failure), keep the output in SAFE state (QSV closed), even though when this device in failure is back in normal condition or PT signal is back in NORMAL state. This STA output **MUST** remain in SAFE state until "Reset command" is applied via STA's MR connection.
b) Include input failure detection, to be capable to detect when the input signal from PT and/or input isolators is in failure state (NAMUR NE 43),
c) But **DO NOT** trip the related QSV valve,
d) Indicate "CommonLS" and DCS (Console Operator) that a "Detected Failures" happened, via the "Fault Relay" contact, and
e) Apply automatically MOS functionality. Refer to section 4.2.15, in document (reference [3]) 0418D20SD04 Safeguarding requirements for further MOS information.

Table 4 – Required MOS logics per SIF device, or "Input/Output Channel"

#	Device's Tag	Type	MOS Tag (2) Manual Tag(3)	"Proof Test" Fail/Success Criterion	Device Description	
1	60-PT-511	Initiator	60-MOS-511 60-HS-511	MAINTENANCE personnel shall manually isolate and pressurize 60-PT-511. **(1)** When pressure reaches trip setting, 60-QSV-511 shall reach the fully closed position in less than 15 sec.	**Pipe Run 1 QSV**	Quick shutdown pressure transmitter
	60-XIB-511	Input				Quick shutdown pressure input isolator
	60-STA-511	Logic				Quick shutdown Logic Solver
	60-XOB-511	Output				Quick shutdown pressure output isolator
	60-SOV-511	Output				SOV to Quick shutdown valve
	60-QSV-511	FSE				Quick shutdown valve
2	60-PT-521	Initiator	60-MOS-521 60-HS-521	MAINTENANCE personnel shall manually isolate and pressurize 60-PT-521. (1) When pressure reaches trip setting, 60-QSV-521 shall reach the fully closed position in less than 15 sec.	**Pipe Run 2 QSV**	Quick shutdown pressure transmitter
	60-XIB-521	Input				Quick shutdown pressure input isolator
	60-STA-521	Logic				Quick shutdown Logic Solver
	60-XOB-521	Output				Quick shutdown pressure output isolator
	60-SOV-521	Output				SOV to Quick shutdown valve
	60-QSV-521	FSE				Quick shutdown valve
3	60-PT-531	Initiator	60-MOS-531 60-HS-531	MAINTENANCE personnel shall manually isolate and pressurize 60-PT-531. (1) When pressure reaches trip setting, 60-QSV-531 shall reach the fully closed position in less than 15 sec.	**Pipe Run 3 QSV**	Quick shutdown pressure transmitter
	60-XIB-531	Input				Quick shutdown pressure input isolator
	60-STA-531	Logic				Quick shutdown Logic Solver
	60-XOB-531	Output				Quick shutdown pressure output isolator
	60-SOV-531	Output				SOV to Quick shutdown valve
	60-QSV-531	FSE				Quick shutdown valve
4	60-PT-541	Initiator	60-MOS-541 60-HS-541	MAINTENANCE personnel shall manually isolate and pressurize 60-PT-541. (1) When pressure reaches trip setting, 60-QSV-541 shall reach the fully closed position in less than 15 sec.	**Pipe Run 4 QSV**	Quick shutdown pressure transmitter
	60-XIB-541	Input				Quick shutdown pressure input isolator
	60-STA-541	Logic				Quick shutdown Logic Solver
	60-XOB-541	Output				Quick shutdown pressure output isolator
	60-SOV-541	Output				SOV to Quick shutdown valve
	60-QSV-541	FSE				Quick shutdown valve

#	Device's Tag	Type	MOS Tag (2) Manual Tag(3)	"Proof Test" Fail/Success Criterion	Device Description	
5	60-PT-510	Initiator	60-MOS-510 60-HS-510	MAINTENANCE personnel shall manually isolate and pressurize 60-PT-510. (1) When pressure reaches trip setting, 60-ESV-510 shall reach the fully closed position in less than 15 sec.	Pipe Run 1 ESV	Emergency shutdown pressure transmitter
	60-XIB-510	Input				Emergency shutdown pressure input isolator
	IC-60-PT-510	Input				Emergency shutdown pressure input card
	CommonLS	Logic				Emergency shutdown Logic Solver
	OC-60-PT-510	Input				Emergency shutdown pressure Output card
	60-XOB-510	Output				Emergency shutdown pressure output isolator
	60-SOV-510	Output				SOV to Emergency shutdown valve
	60-ESV-510	FSE				Emergency shutdown valve
6	60-PT-520	Initiator	60-MOS-520 60-HS-520	MAINTENANCE personnel shall manually isolate and pressurize 60-PT-520. (1) When pressure reaches trip setting, 60-ESV-520 shall reach the fully closed position in less than 15 sec.	Pipe Run 2 ESV	Emergency shutdown pressure transmitter
	60-XIB-520	Input				Emergency shutdown pressure input isolator
	IC-60-PT-520	Input				Emergency shutdown pressure input card
	CommonLS	Logic				Emergency shutdown Logic Solver
	OC-60-PT-520	Input				Emergency shutdown pressure Output card
	60-XOB-520	Output				Emergency shutdown pressure output isolator
	60-SOV-520	Output				SOV to Emergency shutdown valve
	60-ESV-520	FSE				Emergency shutdown valve
7	60-PT-530	Initiator	60-MOS-530 60-HS-530	MAINTENANCE personnel shall manually isolate and pressurize 60-PT-530. (1) When pressure reaches trip setting, 60-ESV-530 shall reach the fully closed position in less than 15 sec.	Pipe Run 3 ESV	Emergency shutdown pressure transmitter
	60-XIB-530	Input				Emergency shutdown pressure input isolator
	IC-60-PT-530	Input				Emergency shutdown pressure input card
	CommonLS	Logic				Emergency shutdown Logic Solver
	OC-60-PT-530	Input				Emergency shutdown pressure Output card
	60-XOB-530	Output				Emergency shutdown pressure output isolator
	60-SOV-530	Output				SOV to Emergency shutdown valve
	60-ESV-530	FSE				Emergency shutdown valve
8	60-PT-540	Initiator	60-MOS-540 60-HS-540	MAINTENANCE personnel shall manually isolate and pressurize 60-PT-540. (1) When pressure reaches trip setting, 60-ESV-540 shall reach the fully closed position in less than 15 sec.	Pipe Run 4 ESV	Emergency shutdown pressure transmitter
	60-XIB-540	Input				Emergency shutdown pressure input isolator
	IC-60-PT-540	Input				Emergency shutdown pressure input card
	CommonLS	Logic				Emergency shutdown Logic Solver
	OC-60-PT-540	Input				Emergency shutdown pressure Output card
	60-XOB-540	Output				Emergency shutdown pressure output isolator
	60-SOV-540	Output				SOV to Emergency shutdown valve
	60-ESV-540	FSE				Emergency shutdown valve

Note 1: Signal change **MUST BE** tested above and below trip setting value.

Note 2: Only one(1) MOS can be "Activated" at the time, or none if other MOS are already activated in the same "MOS Group".

Note 3: Tag of soft-button that ONLY shall be available for Console Operator when the MOC tag is activated. Console Operator can use this sift-button to manually close the associated safety valve.

5.16.2 "Initiators" and Input isolators to trip ESVs

The devices:

- PTs 60-PT-510/520/530/540,
- Input isolators 60-XIB-510/520/530/540, and

shall be configured to set the device output in SAFE state when a device "Diagnostics" detects that a "Detected Failure" occurred. This failure condition shall be communicated up to the "CommonLS" according to NAMUR NE 43.

This means that when a "Detected Failure" happens in any of the above devices, "CommonLS" shall:

a) Indicate DCS (Console Operator) that a "Detected Failures" happened in any of the related devices in the input channel.

b) **DO NOT** trip the related ESV valve, and

c) Apply automatically MOS functionality. Refer to section 4.2.15, in document (reference [3]) 0418D20SD04 Safeguarding requirements for further MOS information.

5.16.3 "CommonLS" and respective Input/Output cards required diagnostics

The "Common Logic Solver" (CommonLS) and respective Input/Output cards shall include:

a) "Fault detection capabilities" (Diagnostics).

b) Pre-configured functionality to allow:
   - "CommonLS" to make decisions according to "Diagnostic" results.
   - To show (or transmit) statuses in DCS (Console Operator), about operation and "Diagnostic" statuses of all SIF devices connected to "CommonLS".

ONLY the input card:

c) **SHALL NOT** trip the related safety valve when a "Detected Failure" occurs in the same input card, or as described in previous sections 5.16.1 and 5.16.2. In this case, MOS automatically applies where it is required.

d) **SHALL NOT** trip the related safety valve when a "Detected Failure" occurs in the associated "Initiator" or input isolator (NAMUR NE 43).

ONLY the "Common Logic Solver" (CommonLS) shall include:

e) Additional circuitry to allow this device to perform the 1oo1D "Decision Logic".

f) To trip ALL LDS's safety valves when a "Detected Failure" occurs in the "CommonLS".

ONLY the CommonLS's Output cards shall include:

g) Additional circuitry to allow this device to perform the 1oo1D "Decision Logic".

h) To trip the related ESV valve when a "Detected Failure" occurs in the output card.

For CommonLS's Output cards related to High Priority Trip 60-SIF-510:

i) Same requirements for other output cards in 60-SIF-500 apply.

j) In addition, when the STA module opens its output circuit (set output in SAFE state) to close the related QSV valve, the "CommonLS" is notified when the related High Priority Trip output card detects that the output circuit is opened.

5.16.4 Output isolators' required diagnostics

Since "Diagnostcs" in devices 60-XOB-510/520/530/540 or 60-XOB-511/521/531/541 **CANNOT** avoid a "Spurious Trip" when a "Safe Detected" failure occurs in the referred isolator, then design decision is to configure ALL "Output Isolators" to trip when a "Detected Failure" occurs (Safe or Dangerous) in the failed isolator.

In this way:

a) The output isolator in failure shall De-Energize output (SAFE state), to close the respective safety valve 60-ESV-510/520/530/540 or 60-QSV-511/521/531/541.

b) Console Operator is notified via direct connection to DCS.

c) Both QSV and ESV valves in the same pipe run shall close. Refer to sections 5.3, 5.9 and 5.15 for further information.

d) "Reset Logic" is applied to keep in SAFE state (closed valve):

   - Isolator that was in failure, when it is fixed and back in normal operation, and
   - The other isolator in the same pipe run. Refer to sections 5.3, 5.9 and 5.15 for further information.

   Refer to references [3] and [4] for "Reset function" further description.

e) It is the Console Operator responsibility to put back in operation the affected pipe run, by pressing related "Reset Button" to release "Reset Logic".

NOTE: implementation shall be able to notify Console Operator (DCS) which "Output Isolator" failed, and which safety valve was trip first.

5.17 Maintenance provisions

Refer to:

- Table 5 for 60-SIF-500 description of basic facilities for MAINTENANCE.
- Section 4.2.17, document (reference [4]) 0418D20SD04 Safeguarding requirements for further information.

60-SIF-500 installation shall be done in such a way that:

1) When a pipe run is "Out Of Service" (OOS), MAINTENANCE personnel shall be able to manually command Open/Close of the pipe run QSV and ESV valves independently.

2) Power supply shall come from the same source for "Common Logic Solver" (CommonLS) and the "Safe Trip Alarm" (STA, Logic Solver) modules. If power supply fails, or it is cut for maintenance purposes, then both "CommonLS" and STA modules' outputs will be set in SAFE state.

3) In addition, a breaker shall be installed for MAINTENANCE purposes to supply power to each STA module, to allow to cut STA power supply independently of the "CommonLS".

4) To power up "CommonLS" and ALL STA modules 60 STA 511/521/531/541 at the same time.

   STA module shall be configured to retain output in SAFE state (De-Energized) for 5 min after STA power up. In this way, it is guarantee that all quick shutdown valve will remain in SAFE state after "CommonLS" and STA modules power up.

5) To power up first the "CommonLS", and after a delay of about 5.0 min to power up the STA modules. This requirement will guarantee that ALL quick shutdown valves 60-QSV-511/521/531/541 remain in SAFE state after power up.

During normal operation ALL LDS's safety valves are opened. Nevertheless, ONLY one of the pipe run can be set "Out Of Service" (OOS) for MAINTENANCE purposes, isolated and safety valves closed. MAINTENANCE shall be able to command position of safety valves in this condition.

NOTE: it is MAINTENANCE and OPERATION responsibility to leave the pipe run safety valves in the closed position (SAFE state) before clear isolation and set pipe run back in normal operation.

Table 5 – 60-SIF-500 description of basic facilities for MAINTENANCE

#	Device's Tag	Type	MOS Tag (2)(3)	OSS Tag (1)(5) Reset button Tag		Remarks
1	60-PT-511	Initiator	60-MOS-511	60-OOS-511 60-HS-511	Pipe Run 1 QSV	Longer time MAINTENANCE than MTTR can be applied after "Out Of Service" (OOS) status activation
	60-XIB-511	Input				
	60-STA-511	Logic				
	60-XOB-511	Output				
	60-SOV-511	Output				
	60-QSV-511	FSE				
2	60-PT-510	Initiator	60-MOS-510		Pipe Run 1 ESV	
	60-XIB-510	Input				
	IC-60-PT-510	Input				
	CommonLS	Logic				
	OC-60-PT-510	Input				
	60-XOB-510	Output				
	60-SOV-510	Output				
	60-ESV-510	FSE				
3	60-PT-521	Initiator	60-MOS-521	60-OOS-521 60-HS-521	Pipe Run 2 QSV	Longer time MAINTENANCE than MTTR can be applied after "Out Of Service" (OOS) status activation
	60-XIB-521	Input				
	60-STA-521	Logic				
	60-XOB-521	Output				
	60-SOV-521	Output				
	60-QSV-521	FSE				
4	60-PT-520	Initiator	60-MOS-520		Pipe Run 2 ESV	
	60-XIB-520	Input				
	IC-60-PT-520	Input				
	CommonLS	Logic				
	OC-60-PT-520	Input				
	60-XOB-520	Output				
	60-SOV-520	Output				
	60-ESV-520	FSE				

#	Device's Tag	Type	MOS Tag (2)(3)	OSS Tag (1)(5) Reset button Tag		Remarks
5	60-PT-531	Initiator	60-MOS-531	60-OOS-531 60-HS-531	Pipe Run 3 QSV	Longer time MAINTENANCE than MTTR can be applied after "Out Of Service" (OOS) status activation
	60-XIB-531	Input				
	60-STA-531	Logic				
	60-XOB-531	Output				
	60-SOV-531	Output				
	60-QSV-531	FSE				
6	60-PT-530	Initiator	60-MOS-530		Pipe Run 3 ESV	
	60-XIB-530	Input				
	IC-60-PT-530	Input				
	CommonLS	Logic				
	OC-60-PT-530	Input				
	60-XOB-530	Output				
	60-SOV-530	Output				
	60-ESV-530	FSE				
7	60-PT-541	Initiator	60-MOS-541	60-OOS-541 60-HS-541	Pipe Run 4 QSV	Longer time MAINTENANCE than MTTR can be applied after "Out Of Service" (OOS) status activation
	60-XIB-541	Input				
	60-STA-541	Logic				
	60-XOB-541	Output				
	60-SOV-541	Output				
	60-QSV-541	FSE				
8	60-PT-540	Initiator	60-MOS-540		Pipe Run 4 ESV	
	60-XIB-540	Input				
	IC-60-PT-540	Input				
	CommonLS	Logic				
	OC-60-PT-540	Input				
	60-XOB-540	Output				
	60-SOV-540	Output				
	60-ESV-540	FSE				

Note 1: OOS tag shall be "Activated" to avoid MOS shutdown after MTTR.

Note 2: Only one(1) MOS can be "Activated" at the time, or none if other MOS are already activated in the same "MOS Group".

Note 3: Above "Note 2" DOES NOT apply for MOS AUTOMATIC activation. Refer to section 4.2.15, in document (reference [3]) 0418D20SD04 Safeguarding requirements for further MOS information.

Note 4: Proper working permits' management and implementation of Lock-out of hand valves **MUST APPLY** to keep these hand valves in the required position during normal operation, to allow 60-SIF-500 to execute action on demand.

MANINTENANCE can be applied to one pipe run while the CPP is in normal operation, **BUT** ONLY when the other three(3) are in normal operation as well.

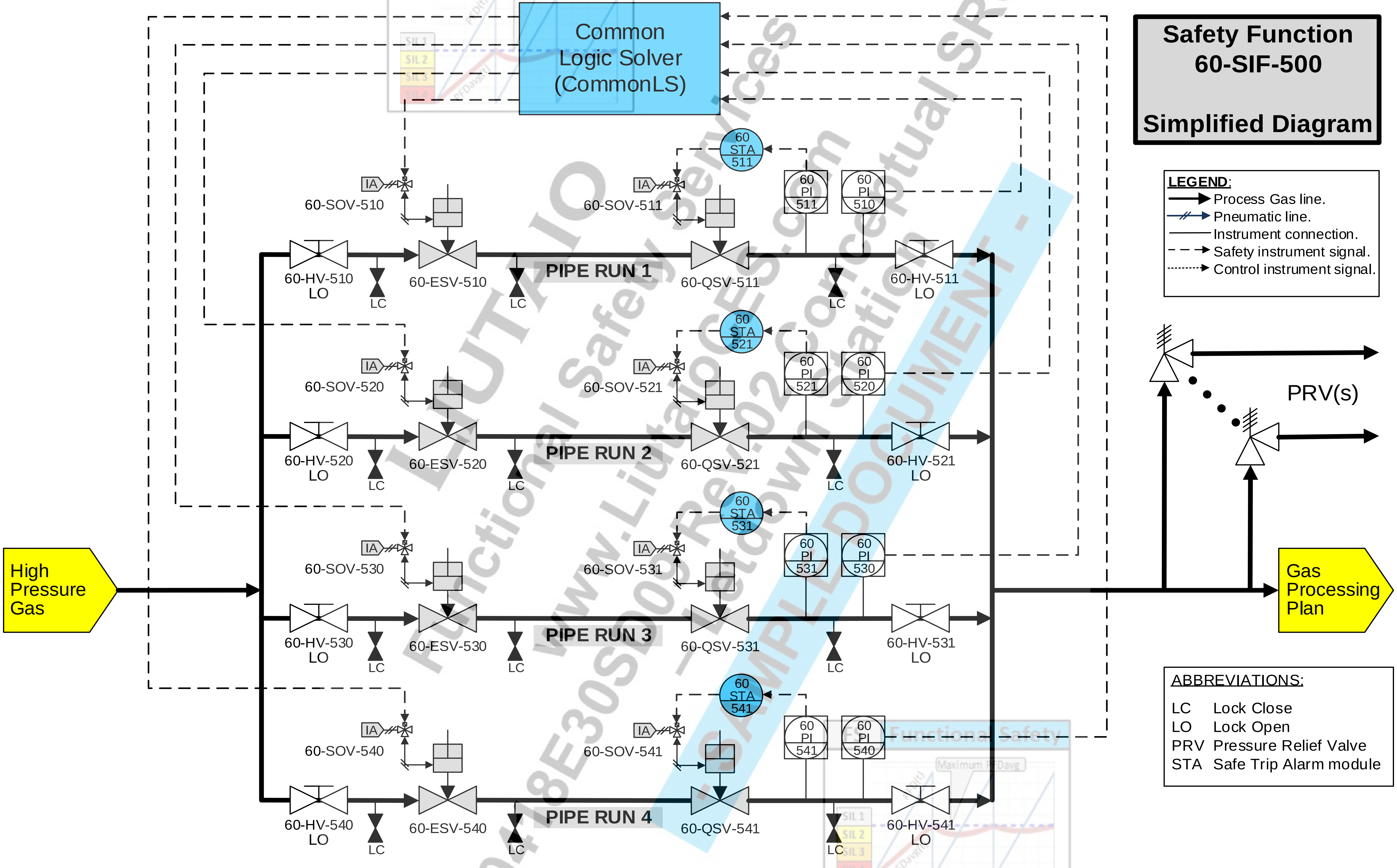
MAINTENANCE can be applied to all instruments and physical pipe run between the isolation valves.

Before applying MAINTENANCE to a pipe run, ALL related SAFETY and PERMISSION procedures **MUST BE** completed and approved. Next, the related pipe run can be set OOS (see Table 5)

5.18 Adjustments and Modifications according to operation modes and/or the project phases

N/A

APPENDIX A – 60-SIF-500 GPP high-pressure protection. Letdown Station (LDS) simplified diagram



Safety Function 60-SIF-500

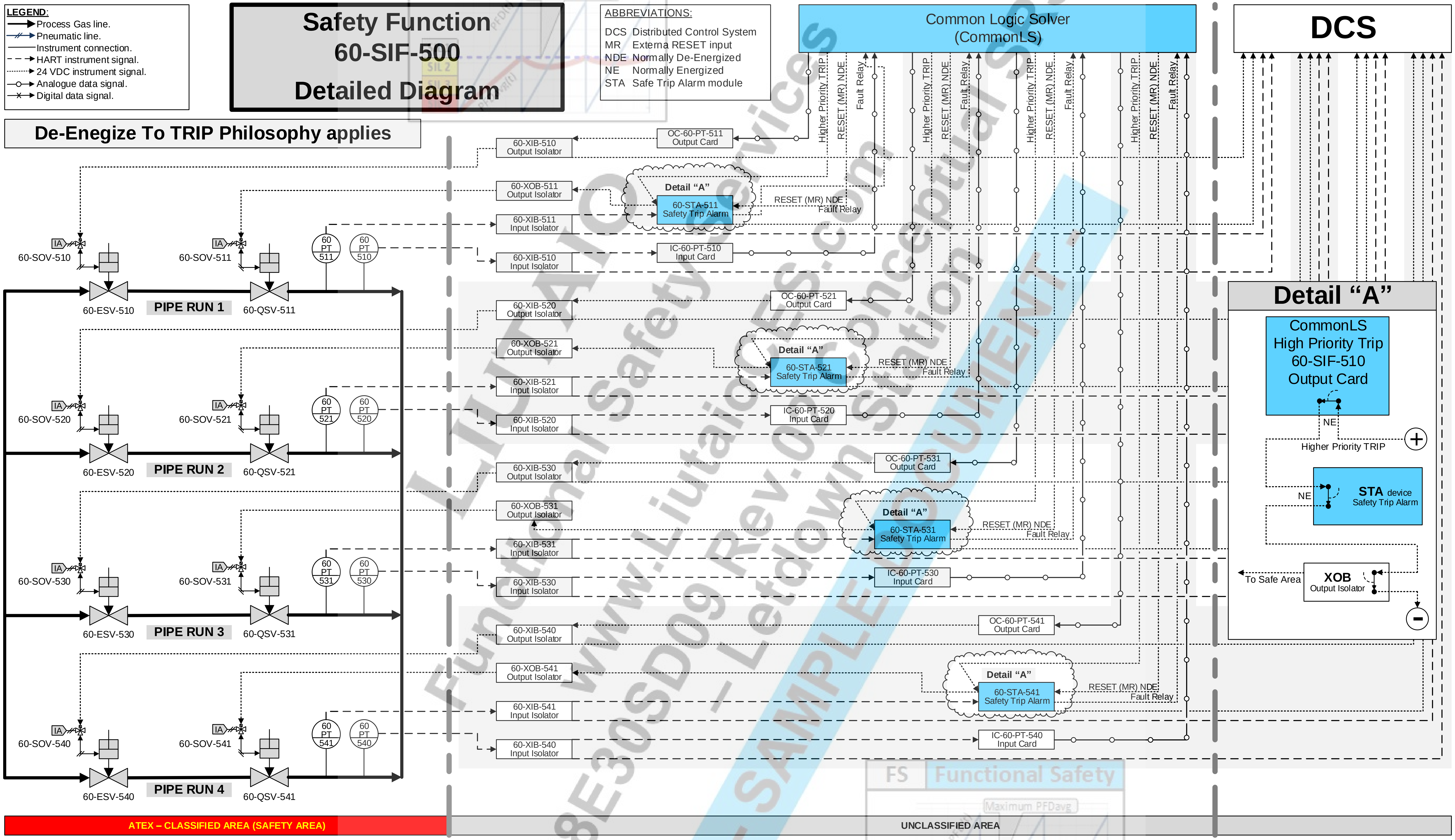
Simplified Diagram

LEGEND:
- Process Gas line.
- Pneumatic line.
- Instrument connection.
- Safety instrument signal.
- Control instrument signal.

ABBREVIATIONS:

LC	Lock Close
LO	Lock Open
PRV	Pressure Relief Valve
STA	Safe Trip Alarm module

APPENDIX B – 60-SIF-500 GPP high-pressure protection. SIF detailed diagram



LEGEND:
- Process Gas line.
- Pneumatic line.
- Instrument connection.
- HART instrument signal.
- 24 VDC instrument signal.
- Analogue data signal.
- Digital data signal.

Safety Function 60-SIF-500 Detailed Diagram

ABBREVIATIONS:

DCS	Distributed Control System
MR	Externa RESET input
NDE	Normally De-Energized
NE	Normally Energized
STA	Safe Trip Alarm module

De-Enegize To TRIP Philosophy applies

Common Logic Solver (CommonLS)
DCS
Higher Priority TRIP
RESET (MR) NDE
Fault Relay
60-XIB-510 Output Isolator
OC-60-PT-511 Output Card
60-XOB-511 Output Isolator
Detail "A"
60-STA-511 Safety Trip Alarm
60-XIB-511 Input Isolator
60-XIB-510 Input Isolator
IC-60-PT-510 Input Card
60-SOV-510
60-SOV-511
IA
60 PT 511
60 PT 510
60-ESV-510
PIPE RUN 1
60-QSV-511
60-XIB-520 Output Isolator
OC-60-PT-521 Output Card
60-XOB-521 Output Isolator
60-STA-521 Safety Trip Alarm
60-XIB-521 Input Isolator
60-XIB-520 Input Isolator
IC-60-PT-520 Input Card
60-SOV-520
60-SOV-521
60 PT 521
60 PT 520
60-ESV-520
PIPE RUN 2
60-QSV-521
60-XIB-530 Output Isolator
OC-60-PT-531 Output Card
60-XOB-531 Output Isolator
60-STA-531 Safety Trip Alarm
60-XIB-531 Input Isolator
60-XIB-530 Input Isolator
IC-60-PT-530 Input Card
60-SOV-530
60-SOV-531
60 PT 531
60 PT 530
60-ESV-530
PIPE RUN 3
60-QSV-531
60-XIB-540 Output Isolator
OC-60-PT-541 Output Card
60-XOB-541 Output Isolator
60-STA-541 Safety Trip Alarm
60-XIB-541 Input Isolator
60-XIB-540 Input Isolator
IC-60-PT-540 Input Card
60-SOV-540
60-SOV-541
60 PT 541
60 PT 540
60-ESV-540
PIPE RUN 4
60-QSV-541
Detail "A"
CommonLS High Priority Trip 60-SIF-510 Output Card
NE
Higher Priority TRIP
+
STA device Safety Trip Alarm
NE
XOB Output Isolator
To Safe Area
−
ATEX – CLASSIFIED AREA (SAFETY AREA)
UNCLASSIFIED AREA